



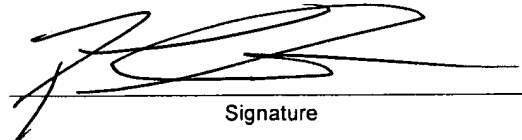
Doc Code: AP.PRE.REQ

PTO/SB/33 (07/05)

Approved for use through xx/xx/200x. OMB 0651-00xx
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PRE-APPEAL BRIEF REQUEST FOR REVIEW		Docket Number (Optional) 50588/360	
I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR on _____ Signature _____ Typed or printed name _____	Application Number 09/930,784		Filed 08/15/2001
	First Named Inventor William M. Gillon		
	Art Unit 2137	Examiner Nadia Khoshnoodi	
<p>Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.</p> <p>This request is being filed with a notice of appeal.</p> <p>The review is requested for the reason(s) stated on the attached sheet(s). Note: No more than five (5) pages may be provided.</p> <p>I am the</p> <p><input type="checkbox"/> applicant/inventor.</p> <p><input type="checkbox"/> assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)</p> <p><input checked="" type="checkbox"/> attorney or agent of record. Registration number 43,548</p> <p><input type="checkbox"/> attorney or agent acting under 37 CFR 1.34. Registration number if acting under 37 CFR 1.34 _____</p> <p>NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.</p>			
<p><input type="checkbox"/> *Total of _____ forms are submitted.</p>			



Signature

Kory D. Christensen

Typed or printed name

(801) 328-3131

Telephone number

7/13/06

Date

This collection of information is required by 35 U.S.C. 132. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11, 1.14 and 41.6. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



Application No. 09/930,784

Docket No. 50588/360
Digeo Ref. P074

Pursuant to the Pre-Appeal Brief Conference Pilot Program, Applicants request review of the rejection of claims 1-5 and 11-20 in the above-referenced application. Clear errors in fact have been made, and essential elements required to establish a *prima facie* rejection are missing. In the Office Action mailed March 14, 2006 ("Office Action"), claims 1-5 and 11-20 were rejected based on U.S. Patent No. 6,563,155 to Akiyama et al. ("Akiyama") and U.S. Patent No. 6,154,206 to Ludtke ("Ludtke").

1. Akiyama and Ludtke do not teach or suggest encrypting a group of multimedia channels using a first type of encryption and encrypting the same group of multimedia channels using a second type of encryption to produce first and second groups of encrypted multimedia channels.

Claim 1, as it currently reads in the application, includes, among other things:

encrypting a group of multimedia channel keys using a first type of encryption to produce a first group of encrypted multimedia channel keys;

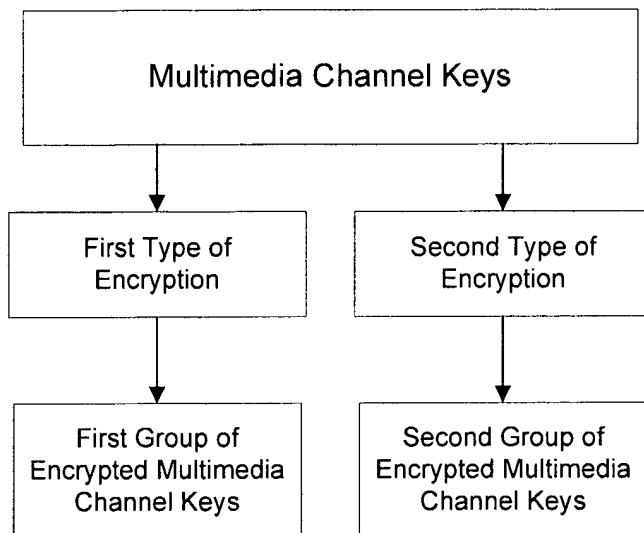
encrypting said group of multimedia channel keys using a second type of encryption to produce a second group of encrypted multimedia channel keys . . .

New multimedia receivers may use advanced types of encryption as compared to older multimedia receivers. The different types of encryption are not interchangeable. For example, the older legacy multimedia receivers cannot decrypt the more advanced types of encryption that the new multimedia receivers are able to decrypt.

According to the claimed invention, a group of multimedia channel keys is encrypted using two different types of encryption to produce two different groups of encrypted multimedia

channel keys. Thus, *the same group of unencrypted multimedia channel keys is encrypted two different ways.*

After encryption with the first and second types, two encrypted versions of the same multimedia channel keys exist. Each version includes the content of the group of multimedia channel keys, but with a different encryption. The claimed process may be illustrated as follows:

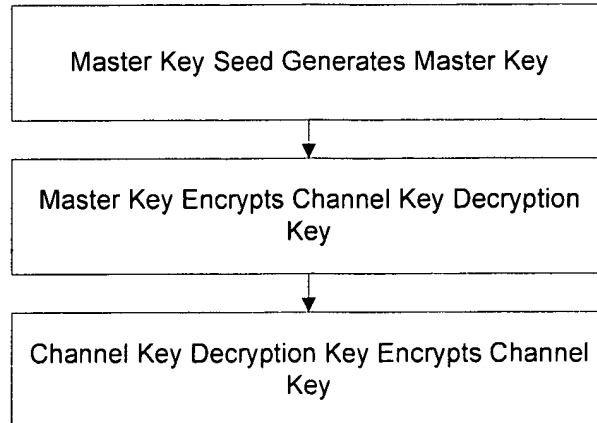


Claim 1 recites *encrypting said group of multimedia channel keys using a second type of encryption.* Thus, it is the same group of unencrypted multimedia channel keys that is encrypted using a second type. Claim 1 does not recite using a second type of encryption to encrypt the already encrypted multimedia channel keys. Interpreting claim 1 in this manner is clear error.

Akiyama does not teach the encryption of the *same group of unencrypted channel keys* using two different forms of encryption. Rather, Akiyama teaches encryption of a channel key by a channel key decryption key, which is encrypted by master key, which is generated by a master key seed. Akiyama, column 8, lines 50-53, column 27 lines 4-51, and Figure 32.

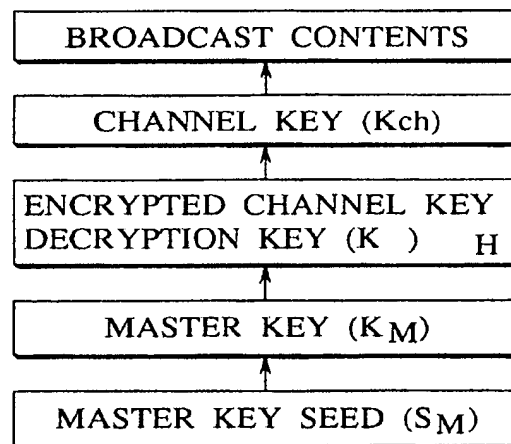
Akiyama recites that it uses a four-stage encryption mechanism, but Akiyama has absolutely no teaching of encrypting the original, unencrypted channel key according to two different encryption types.

The process of Akiyama may be illustrated as follows:



This is supported by Figure 32 of Akiyama, which is also illustrated as follows:

FIG.32



Akiyama teaches the encryption of a channel key K_{ch} by a key K_H , which is in turn encrypted by another key K_M . This does not teach or suggest that the original channel key K_{ch} is encrypted using a first version and then the original channel key K_{ch} is again encrypted using a second version.

It appears that the Office Action may suggest that Akiyama teaches the encryption of channel key K_{ch} by key K_H and then the now-encrypted key K_{ch} is again encrypted by key K_M . Such a teaching, whether present in Akiyama or not, does not disclose the claimed invention.

Claim 1 does not recite encrypting an already encrypted channel key. Such a double serial encryption is not claimed or considered in the pending application. In the present application, two different encryption versions each encrypt the *original* channel key. When claim 1 recites *encrypting said group of multimedia channel keys using a second type of encryption*, it is the same group of originally introduced multimedia channel keys, not a group of encrypted channel keys. To read claim 1 as a double serial encryption is clear error.

Claim 11 presently recites, among other things, “transmitting decryption keys for decrypting said multimedia channels.” Thus, the decryption keys are channel keys. Claim 11 further recites “said decryption keys encrypted in both a first encryption format and a second encryption format.” Whether doubly-serially encrypted or not, Akiyama only discloses transmitting channel keys in a single encryption format.

Ludtke was not cited in the Office Action for the claimed limitations discussed above, but also fails to teach encrypting channel keys using first and second encryption formats.

2. Akiyama and Ludtke do not teach or suggest concurrently transmitting first and second groups of encrypted multimedia channel keys to multimedia subscribers having multimedia receivers.

Claim 1 includes, in its present form:

concurrently transmitting said first group of encrypted multimedia channel keys with said second group of multimedia channel keys to a plurality of multimedia subscribers having multimedia receivers . . .

For this claimed limitation, the Office Action cites to Ludtke. Ludtke discloses that main broadcast data (DBS) may be delivered at a different frequency than OOB data. Ludtke column 7, lines 2-17. The OOB data may be used to decrypt the DBS. Ludtke, column 3, lines 45-47.

Thus, Ludtke discloses that OOB data and DBS may be transmitted at different frequencies. Ludtke discloses the use of multiple tuner subunits to receive signals in different frequency ranges. Ludtke, column 7, lines 9-11. The Applicants acknowledge that the concurrent transmission of a channel key and multimedia content is known.

However, Ludtke fails to teach the concurrent transmission of two groups of encrypted channel keys for the same original channel keys. There is absolutely no teaching or suggestion in Ludtke of concurrently transmitting two different groups of encrypted OOB data for the same unencrypted OOB data. Indeed, there is no purpose for so doing in Ludtke as Ludtke is not concerned with receiving the same channel key for different versions of multimedia receivers.

Akiyama also fails to teach concurrently transmitting two different groups of encrypted channel keys for the same unencrypted channel keys. Akiyama discloses the use and transmission of channel key K_{ch} , channel key decryption key K_H , and master key K_M , but not the simultaneous transmission of two encrypted channel keys originating from the same channel key. Instead, Akiyama teaches serial decryption of a channel key K_{ch} which may increase security but does not teach concurrent transmission of two different encrypted versions containing the same channel key.

Conclusion

Akiyama and Ludtke fail to teach the discussed limitations, which is not surprising since neither reference is concerned with the incompatibility of older and newer multimedia receivers to decrypt channel keys. Based at least on the foregoing, claims 1 and 11 are allowable over the art that has been cited and applied by the Examiner. Further, claims 2-5 and 12-20 are allowable by virtue of their dependency on claims 1 and 11 respectively. Applicants therefore request withdrawal of the rejections and allowance of the pending application at an early date.